UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/554,275	10/25/2005	Andreas Lindinger	2004P12244WOUS	2989

29177 7590 09/10/2008

BELL, BOYD & LLOYD, LLP
P.O. BOX 1135
CHICAGO, IL 60690

EXAMINER	
NGUYEN, TRONG H	

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
09/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/554,275	LINDINGER ET AL.	
	Examiner	Art Unit	
	TRONG NGUYEN	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 October 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5* is/are rejected.

7)☒ Claim(s) *5* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 October 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/09/2007 and 05/19/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application numbered 10554275 filed on 10/25/2005 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in 37 C.F.R. 1.63.

Priority

As required by M.P.E.P. 201.14(c), acknowledgement is made of applicant's claim for priority based on application filed on August 03, 2004 (DE 10 2004 037 801.0)

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which have been placed of record in the file.

Should applicant desire to obtain the benefit of foreign priority under 35 U.S.C. 119(a)-(d) prior to declaration of an interference, a certified English translation of the foreign application must be submitted in reply to this action. 37 CFR 41.154(b) and 41.202(e).

Failure to provide a certified translation may result in no benefit being accorded for the non-English application.

Information Disclosure Statement

3. The information disclosure statements (IDS) submitted on 05/19/2008 is in compliance with the provisions of 37 C.F.R. 1.97 and is being considered by the examiner. In the information disclosure statement submitted on 03/09/2007, item listed as RANKL W. et al.: "AUTHENTISIERUNG" fails to comply with 37 CFR 1.98(a)(3) because an English translation was not provided by the applicant and thus this item will not be considered by the examiner. However, other remaining items are in compliance with the provisions of 37 C.F.R. 1.97 and therefore are being considered by the examiner.

Drawings

4. The drawings are objected to because in Fig. 1, step 13, "TOES" appears to be a misspell of "TDES" and in Fig. 2, step 24, a left to right arrow which is used to indicate the transfer of Cert. Lev. 1 from T2 to T1 is missing. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement

sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

5. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed.

The following title is suggested: Method for Secure Data Transmission between a Tachograph and Memory Card.

Claim Objections

6. Claim **5** is objected to because of the following informalities: Claim **5** recites "n = 3" in line 2. There is insufficient antecedent basis for this limitation in the claim. It is believed that claim **5** was intended to refer to "n" in claim **4**. Accordingly, applicant might consider changing the dependency of claim **5** from claim **1** to claim **4**. Appropriate correction is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims **1-3** are rejected under 35 U.S.C. 103(a) as being unpatentable over Rune US 5,850,444 (hereinafter "Rune"), in view of Mutz US 4,644,368 (hereinafter "Mutz"), and further in view of Hsu et al. US 2004/0063438 (hereinafter "Hsu").

Regarding claim **1**, Rune discloses "A method for secure data transmission between a first subscriber and second subscribers" and "having at least one respective data store" as ["a method and apparatus for encrypting radio traffic between terminals and a mobile communications network" (Col. 1, lines 8-10)] "wherein the first subscriber has a memory which stores a particular number of entries, each comprising identifiers and associated certificates from the second subscribers" as ["The terminal stores at least one public key in the non-volatile memory. Along with each public key, the terminal also stores a respective expiration date for the key, and a GAN identification character that identifies a specific GAN associated with that key" (Col. 5, lines 36-40). Furthermore, Rune discloses "when a public key is to be transferred from a GAN to a terminal, the key can be transferred with a public key 'certificate' (Col. 10, lines 43-45). It is obvious to the terminal if desired to store certificates associated with public keys for

use in subsequent transmissions as Rune mentioned "This certificate provides proof that the associated public key and the owner of that key are authentic" (Col. 10, lines 45-47)] "fetching an identifier by the first subscriber from the second subscriber" and "comparing by the first subscriber the identifier with the identifiers stored in the memory" as ["The terminal initiates contact by registering with a specific GAN (but not necessarily setting up a call). A processor in the terminal compares the received GAN identifier with the stored identifiers" (Col. 5, lines 42-45)] "if a matching identifier is present, prompting the security certificate associated with the identifier to be a basis for subsequent data transmission" as ["and if a match can be made (and the key has not expired), the processor retrieves the stored public key associated with the identified GAN" (Col. 5, lines 44-47) and "the same public key can be used for all subsequent communications with that GAN" (Col. 6, lines 54-55). By teaching using the retrieved public key in subsequent communications, Rune also teaches using the associated security certificate in subsequent data transmissions such as to verify the authenticity of the public key and/or its owner.] "if no matching identifier is stored in the memory, prompting the first subscriber to perform security certificate verification with the second subscriber" as ["However, in the event that no such match is found, the terminal sends a request for the GAN to transmit a public key" (Col. 5, lines 47-49). In addition, Rune discloses "a problem can arise if an unauthorized user attempts to impersonate a GAN and transmit a public key to the terminal. In that event, as described below, the terminal can be configured to authenticate the received public key and the identity of the GAN. For example, when a public key is to be transferred from a GAN to a terminal, the key can

be transferred with a public key 'certificate'." (Col. 10, lines 38-45). By teaching authenticating the received public key and the identity of the GAN, Rune also teaches verifying the associated certificate accompanying that public key.]

Rune does not specifically disclose "first subscriber being a tachograph in a commercial vehicle and the second subscriber being memory cards", "with a detection time for the security certificate", "updating the detection time for the security certificate to a current system time", and "in the event of verification, storing an entry corresponding to the verified security certificate with a current detection time in the memory with the entry with the oldest detection date being replaced by the new entry if a particular number of entries has already been reached".

Mutz discloses a tachograph for motor vehicles with a microprocessor comprising a time and date generator communicating with a data card.

Mutz and Rune are analogous art because they are in the same field of endeavor of data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to adopt Rune's method of secure data transmission to be used in data communications between other devices such as in communication between a tachograph and memory card by having the tachograph storing identifiers and associated certificates, fetching an identifier from the memory card, comparing this identifier with stored identifiers, and performing certificate verification with the memory card if no match is found. In addition to using continuous numbering and storing personal work-time data records on memory card, Rune's method of secure data

transmission will extensively reduce the "danger of manipulation and loss of driving records" and hence the transmission between the tachograph and memory card will be "more secure from disturbance and counterfeiting (Mutz, Col. 10, lines 24-25 and 41).

Hsu discloses "a MAC-SU list manager 69" which "has multiple entries 102" and the "entry also includes a time stamp 108 corresponding to the time at which the entry was created or updated" (Par. 0051, lines 14-16). Furthermore, Hsu discloses "When the MAC-SU list is full, and the microprocessor needs to install an additional entry, the microprocessor scans the index group to which the new entry applies, finds and deletes the oldest entry (i.e. the entry with the earliest time stamp) in the group, and enters the new entry" (Par. 0056, lines 7-12).

Hsu, Rune, and Mutz are analogous art because they are in the same field of endeavor of data communication.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to enhance the method of data transmission between the tachograph and memory card of Rune in view of Mutz by including a time stamp or detection time for each certificate, updating the detection time to current system time when the certificate is used, and in the process of certificate verification storing an entry corresponding to the verified certificate by replacing the entry with the oldest detection time with the new entry with the current detection time if the particular number of entries has been reached in order to save memory space and "in this manner, the system constantly updates the MAC-SU List to include those user devices that are currently active" (Hsu, Par. 0056, lines 15-17).

Regarding claim **2**, Rune discloses "wherein the identifier is a public key from an RSA method from the second subscriber as ["a mobile terminal stores at least one public key, along with a unique identification character of at least one GAN associated with that public key, in memory location" (Col. 4, lines 16-19) and "the GAN can maintain one or more asymmetric public key/private key pairs. In that event, a so-called 'RSA Algorithm' can be used to create the public key/private key pairs" (Col. 7, lines 1-2). By teaching a unique identification character associated with a public key and using the RSA algorithm to create the public key/private key pairs, Rune also teaches that the unique identifier can be a RSA public key from the second subscriber.]

Regarding claim **3**, Rune discloses "wherein a subsequent data transmission is effected in TDES-encrypted form, with verification of the security certificates being followed by both subscribers sending a random number in encrypted form to the other subscriber and both subscribers independently of one another each using the two random numbers to determine a common key for data transmission using the same algorithm" as ["a so-called Diffie-Hellman 'exponential key exchange' algorithm can be used to let the terminal and the GAN agree on a secret session key" (Col. 9, lines 50-53), "The terminal (118) generates the random number X_T ($1<X_T<q-1$), and computes the value $Y_T=a^{X}{}_T$ mod q. The GAN (e.g., the RNC or base station) generates the random number X_G ($1<X_G<q-1$), and computes the value of $Y_G=a^{X}{}_G$ mod q (Col. 9, line 66-Col.10, line 3), "Y_T and Y_G are transferred unencrypted to the respective GAN and terminal" (Col. 10, lines 6-7). Then, both the terminal and the GAN independently generates the "communications session encryption key" K_S (Col. 10, line 13-14).

Furthermore, Rune discloses "A known symmetric encryption algorithm can be used to encrypt and decrypt the ensuing radio traffic with the secret key, such as, for example, a one, two or three pass Data Encryption Standard (DES) algorithm" (Col. 9, lines 44-47). Though, Rune discloses Y_T and Y_G are transferred unencrypted to the respective GAN and terminal, it is obvious that Y_T and Y_G can be transferred encrypted if one is desired to do so.]

9. Claims **4-5** are rejected under 35 U.S.C. 103(a) as being unpatentable over Rune in view of Mutz, and further in view of Hsu, and further in view of Kostal et al. US 7,308,573 (hereinafter "Kostal").

Regarding claim **4**, Rune in view of Mutz and further in view of Hsu discloses "The method according to claim 1 wherein the verification of the certificate from the first subscriber by the second subscriber " but does not specially disclose "and vice versa" and "comprises the following n number of steps: in the first step, the second subscriber sends the first subscriber a first security certificate which the second subscriber subject to verification using a first public key and in doing so ascertains a second public key, and if the verification results in authenticity then the first step is repeated (n-1) times using a further transmitted security certificate and the second public key ascertained in the previous step instead of the first public key, with a new second public key and a verification result always being obtained."

However, Kostal discloses "The process of validating the digital signatures in a chain" (Col. 15, lines 37-38) wherein "knowledge of the public key corresponding to the private key of the trusted authority is gained, and such public key of the trusted authority

is employed to verify the signature of the root certificate in the chain. Presuming the root certificate signature verifies, then, the public key from the root certificate is obtained and employed to verify the signature of the first intermediate certificate in the chain. The process repeats serially through the chain until every signature thereof is verified" (Col. 16, line 65-Col. 17, line7). By teaching a method of verifying a chain of certificate above, Kostal also teaches a method of verifying multiple certificates from a single subscriber with multiple public/private key pairs and in the process ascertaining the subscriber's public keys. Furthermore, Kostal also teaches that this certificate verification process comprises n number of steps if the user has n number of certificates.

Kostal, Rune, Mutz, and Hsu are analogous art because they are in the same field of endeavor of data transmission and security.

It would have been obvious to a person of ordinary skill in the art at the time of the invention to enhance the method of data transmission between the tachograph and memory card of Rune in view of Mutz, and further in view of Hsu by having both subscribers mutually verify each other's certificates by first verifying all certificates of one subscriber using the method as disclosed by Kostal above and then verify the other subscriber's certificates also using the same method in order to authenticate both subscribers and hence resulting in a stronger security level between the two subscribers.

Regarding claim **5**, for examining purposes, claim **5** will be considered to be dependent on claim **4**. By disclosing the process of verifying multiple certificates in n

number of steps by Kostal, barring any unexpected result, it would have been obvious that the number of steps can be 3 which is one instance of n.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Prior art US 6,782,474 teaches method of secure, remote configuration method between new network devices and management station.

Prior art US 5,371,794 teaches method and apparatus for privacy and authentication in wireless networks.

Prior art US 2004/0059916 teaches a storage device in which processing time of security processes is reduce while assuring safety of the security processes.

Prior art US 5,721,781 teaches smart card and terminal exchanging certificates to authenticate one another.

Prior art US 6,772,331 teaches method and system for enabling wireless devices to be paired by a user.

Prior art US 6,198,996 teaches an onboard computer to control aspects of a vehicle used in combination with a smart card key.

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRONG NGUYEN whose telephone number is (571)270-7312. The examiner can normally be reached on Monday through Thursday 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TN

/THOMAS PHAM/
Supervisory Patent Examiner, Art Unit 4148